Comment Report

STATEWIDE POLICY – INFORMATION SECURITY PROGRAMS

FEBRUARY 23, 2010

Scope:

This report contains the comments and responses for the statewide review of the *Statewide Policy: Information Security Programs*, which was available for review January 12th to February 5th, 2010.

Executive Summary

The purpose of this document is to:

1. Publish received comments,
2. indicate status of proposed changes, and
3. respond to each comment with recommendations.

Comments were received from three agencies, over the period of January 12st through February 8rd. The comments were in the following areas:

4. Comments regarding implementation; specifically required resources and funding. These have been addressed herein.
5. Technical question regarding the version number of a referenced document. Recommended corrected language is included below.

The respondents did not appear to include agency policy-makers - those individuals nominally responsible for implementing policy (i.e., directors, administrators, etc.); and *policy-level* concerns were not detected within the comments. There is recognition among the respondents of the strategic nature of aligning security programs to the National Institute of Standards and Technology (NIST) Risk Management Framework.

The upshot being that we are not aware of any policy-maker concerns stemming from this policy, other than funding.

The recommendation from the policy proponent to the State of Montana Chief Information Officer is to approve the policy based on the response herein.

Comments/Feedback with Response

Item	Comment/Suggestion	Response/ Disposition	Status
1.	**COMMENT:** The policy requires the <responding department 1> implement an Information Security Program which is aligned and integrated with the National Institute of Standards and Technology (NIST) Special Publication 800-39 Managing Risk from Information Systems. NIST SP 800-39 requires the following components in a Security Program: • Security planning • Security policy • Security awareness and training • Risk assessments • Performance management To be in compliance with this policy the <responding department 1> would have to increase their security staff by 2 FTE.	**RESPONSE:** Concur with the <responding department's> need to apply resources. All laws, regulations, policies, standards, procedures, and other sources of requirements result in expenditure in some combination of the "five scarce resources": money, materials, machines, methods and people. All business, including the business of government requires that managers prioritize the available resources to achieve mission success. The NIST guidance anticipates the fact that resources will be required, allocated, and expended, and provides the mechanism to support requests for resources and support, via the Risk Management Framework (reference NIST SP800-39 Managing Risk From Information Systems). The Risk Management Framework results in deliverables that are required to satisfy federal and State of Montana funding processes, such as HB10 requirements for security plans. The Risk Management Framework will identify security program needs, which will determine resource requirements. Individual agencies will make informed business decisions to pursue funding or not, and accept the risk stemming from their decisions. The effective date of the policy has been established two and one-half years out in order to afford the agencies time to align their current security program (under §2-15-114, MCA) with NIST guidance. Under this guidance, *agencies can manage their alignment to NIST based on their business capabilities, constraints and restraints.* **RECOMMENDATION:** The policy proponent recommends that the agencies use the resources allocated in support of the program requirements of §2-15-114, MCA, to align their current program to the NIST guidance. Guidance and consultation are available from the Enterprise Information Systems Security Bureau on request.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
2.	**COMMENT:** Without an increase in security staff <responding department 1> could put together a “bare bones” security program. This program would meet the minimum requirements only after many years of development and implementation. A security program with current staffing would be almost all reactive with changes and progress only being made as a response to audit findings.	**RESPONSE:** Concur. Information risk management will require many years of development and implementation, just like any other *management* discipline for key resources. (I.e., budgeting, human resources, safety, asset management, etc.) The State of Montana Legislature recognized this fact by requiring manager roles and security programs with §2-15-114, MCA. The Federal Information Security *Management* Act (FISMA - emphasis added) is the enabling statute mandating the NIST security guidance at the federal level, and is the emerging source of security requirements for federal programs and associated federal expenditures within state programs. FISMA recognizes the fact that information security is a management issue, requiring programs and the attendant investment. Through NIST guidance, FISMA addresses the program and funding aspects of information security. Aligning with the NIST guidance minimizes the risk of non-compliance within federal programs and federally funded state programs; Hence, the policy requirements to use NIST. The proponent estimates that agencies will require five-to-eight EPP cycles (depending on individual agency business requirements, constraints and restraints) to align their current security programs to the NIST guidance. This timeframe will be further influenced by the amount and degree of security controls present in agencies’ current program under §2-15-114, MCA. **RECOMMENDATION:** The policy proponent recommends that the agencies use the resources allocated in support of the program requirements of §2-15-114, MCA, to align their current program to the NIST guidance, recognizing the need for management prioritization of limited resources. Guidance and consultation is available from the Enterprise Information Systems Security Bureau on request.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
3.	**COMMENT:** <Responding department 1> applauds the efforts to make a NIST compliant Security program the standard for the State of Montana and agrees that these standards are a commendable goal. However, unless additional FTE and the funding for them are approved and appropriated this policy constitutes an unfunded mandate.	**RESPONSE:** Non-concur. Taxpayers continue to fund agencies' security programs under §2-15-114, MCA as they have for the last twenty-two years. This is evidenced by agencies having security personnel on staff and historic and ongoing actions to implement security controls. Security personnel salaries are paid and security solutions procured and implemented because of continued funding support. This policy is promulgated under §2-17-534, MCA, to support the agencies' current security programs under §2-15-114, MCA. If agencies have not implemented security programs per §2-15-114, MCA, that is a larger issue not germane to this policy. Agencies may request an exception to this policy; either in whole or in part. But, an exception would not provide relief from other state and federal requirements that have a basis in NIST guidance; or are driven by FISMA, the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry – Data Security Standard (PCI-DSS), etc. Compliance with those requirements would be problematic if agencies' security programs fail to align with NIST guidance. See item 1 above, for a discussion of funding issues. **RECOMMENDATION:** The policy proponent recommends that the agencies use the resources (e.g., funding) allocated in support of the program requirements of §2-15-114, MCA to align their current program to the NIST guidance required by this policy. The policy proponent also recommends that agencies account for their security program expenditures explicitly against mandates (such as §2-15-114, MCA or state/federal programs). This enables agencies to have an informed discussion with executive and legislative authorities about the cost of compliance. Those authorities may then consider how implementation shall be supported, or take other actions, as they deem appropriate.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
4.	**COMMENT:** <Responding department 2> supports and is committed to the Information Security Program which includes risk analysis, mitigation planning and overall security awareness & education. Implementing and maintaining a security program will have an impact to the department which at this time is difficult to identify like staff and budget. The overall results of the department's investment (staff time and other resources) will benefit our customers by avoiding or reducing the costs associated with data security\loss.	**RESPONSE:** Concur. **RECOMMENDATION:** See Response and Recommendation in item 1, above. Going forward, guidance and consultation is available from the Enterprise Information Systems Security Bureau and the Information Security Managers Group to support program, resource, and funding planning.	No Change
5.	**COMMENT:** Question – Section VIII – Requirements of the draft document for the Information Security Policy Instrument says that the agencies shall implement their security program based on NIST guidance and specifically points to NIST SP 800-53, Revision 3. The embedded link brings that document up from the NIST Website. What happens if the document gets revised again? The policy document would be directing the agencies to a non-current document to work from. Should you add that they need to use the most current version of this document and perhaps direct them to NIST's document directory at: http://csrc.nist.gov/publications/PubsSPs.html and have them check for currency?	**RESPONSE:** Good point. As a key living document, NIST SP800-53 will continue to evolve. **RECOMMENDATION:** The following language replaces any reference to a specific version number of all NIST documents referenced within the policy: Agencies shall use the latest publicly available versions of publications referenced within this Policy *at its date of approval*. (Note: Because newer versions of the publications referenced herein become available from time-to-time, each agency is encouraged to stay current by using the most recent versions, as deemed feasible by each agency. Future revisions of this Policy shall reference then currently available versions.)	Change Prose